CLAIMS

What is claimed is:

1. A method for granting access to a protected area of a storage device from a calling process, comprising the steps of:

causing a calling process desiring to gain access to the protected area to locate an interface that permits access to the protected area;

causing the calling process to use the interface to create a trusted relationship between the calling process and system firmware;

once the trusted relationship has been established, allowing the calling process access to retrieve a directory of service areas in the protected area;

allowing access to one or more service areas in the protected area;

processing data contained in the one or more service areas; and

closing the protected area when processing data in the one or more service areas is complete.

2. The method recited in Claim 1 wherein the trusted relationship comprises the steps of:

sending a public key to the system firmware;

modifying the public key using a private key using the system firmware;

causing the calling process to validate the modified key;

causing the system firmware to issues a public key to the calling process;

modifying the public key using the private key using the calling process;

causing the system firmware to validate the new key; and

if the key is not validated, granting not access to the protected area; and

if the key is validated, granting access to the protected area.

3. The method recited in Claim 1 wherein the step of allowing access to the one or more service areas comprises the steps of:

returning a handle from the system firmware to the calling process once the system firmware has learned to trust the calling process;

modifying the handle using the calling process;

returning the modified handle to the system firmware as a part of the retrieve directory request; and

allowing the calling process to locate the desired service area using the information returned by the retrieve directory request.

4. The method recited in Claim 1 wherein the step of allowing access to the one or more service areas comprises the steps of:

returning a handle from the system firmware to the calling process once the system firmware has learned to trust the calling process;

modifying the handle using the calling process;

returning the modified handle to the system firmware as a part of a retrieve directory request; and

if the open request succeeds, causing the system firmware to move a SETMAX boundary to allow access to the requested service area.

5. The method recited in Claim 1 wherein the step of allowing access to the one or more service areas comprises the steps of:

returning a handle from the system firmware to the calling process once the system firmware has learned to trust the calling process;

modifying the handle using the calling process;

returning the modified handle to the system firmware as a part of an open service area with a password request; and

if the open request succeeds, causing the system firmware to move a SETMAX boundary to allow access to the requested service area.

6. The method recited in Claim 1 wherein the step of closing the protected area comprises the step of:

once the calling process has completed its activities in the protected area 27, returning the SETMAX address to its original boundary using a close command.

7. A method for granting access to a protected area of a storage device from a calling process, comprising the steps of:

causing a calling process desiring to gain access to the protected area to locate an interface that permits access to the protected area;

causing the calling process to use the interface to create a trusted relationship between the calling process and system firmware;

once the trusted relationship has been established, allowing access to a one or more service areas in the protected area;

processing data contained in the one or more service areas; and

closing the protected area when the processing in the one or more service areas is complete.

8. The method recited in Claim 7 wherein the trusted relationship comprises the steps of:

sending a public key to the system firmware;

modifying the public key using a private key using the system firmware;

causing the calling process to validate the modified key;

causing the system firmware to issues a public key to the calling process;

modifying the public key using the private key using the calling process;

causing the system firmware to validate the new key; and

if the key is not validated, not granting access to the protected area; and

if the key is validated, granting access to the protected area.

9. The method recited in Claim 7 wherein the step of allowing access to the one or more service areas comprises the steps of:

returning a handle from the system firmware to the calling process once the system firmware has learned to trust the calling process;

modifying the handle using the calling process;

returning the modified handle to the system firmware as a part of the retrieve directory request; and

allowing the calling process to locate the desired service area using the information returned by the retrieve directory request.

10. The method recited in Claim 7 wherein the step of allowing access to the one or more service areas comprises the steps of:

returning a handle from the system firmware to the calling process once the system firmware has learned to trust the calling process;

modifying the handle using the calling process;

returning the modified handle to the system firmware as a part of a retrieve directory request; and

if the open request succeeds, causing the system firmware to move a SETMAX boundary to allow access to the requested service area.

11. The method recited in Claim 7 wherein the step of allowing access to the one or more service areas comprises the steps of:

returning a handle from the system firmware to the calling process once the system firmware has learned to trust the calling process;

modifying the handle using the calling process;

returning the modified handle to the system firmware as a part of an open service area with a password request; and

if the open request succeeds, causing the system firmware to move a SETMAX boundary to allow access to the requested service area.

12. The method recited in Claim 7 wherein the step of closing the protected area comprises the step of:

once the calling process has completed its activities in the protected area 27, returning the SETMAX address to its original boundary using a close command.

13. A method for granting access to a protected area of a storage device from a calling process, comprising the steps of:

causing a calling process desiring to gain access to the protected area to locate an interface that permits access to the protected area;

causing the calling process to use the interface to create a trusted relationship between the calling process and system firmware;

once the trusted relationship has been established, manipulating one or more service areas found in the protected area;

closing the protected area when the processing in the one or more service areas is complete.

14. The method recited in Claim 13 wherein the trusted relationship comprises the steps of:

sending a public key to the system firmware;

modifying the public key using a private key using the system firmware;

causing the calling process to validate the modified key;

causing the system firmware to issues a public key to the calling process;

modifying the public key using the private key using the calling process;

causing the system firmware to validate the new key; and

if the key is not validated, not granting access to the protected area; and

if the key is validated, granting access to the protected area.

15. The method recited in Claim 13 wherein the step of allowing access to the one or more service areas comprises the steps of:

returning a handle from the system firmware to the calling process once the system firmware has learned to trust the calling process;

modifying the handle using the calling process;

returning the modified handle to the system firmware as a part of the retrieve directory request; and

allowing the calling process to locate the desired service area using the information returned by the retrieve directory request.

16. The method recited in Claim 13 wherein the step of allowing access to the one or more service areas comprises the steps of:

returning a handle from the system firmware to the calling process once the system firmware has learned to trust the calling process;

modifying the handle using the calling process;

returning the modified handle to the system firmware as a part of a retrieve directory request; and

if the open request succeeds, causing the system firmware to move a SETMAX boundary to allow access to the requested service area.

17. The method recited in Claim 13 wherein the step of allowing access to the one or more service areas comprises the steps of:

returning a handle from the system firmware to the calling process once the system firmware has learned to trust the calling process;

modifying the handle using the calling process;

returning the modified handle to the system firmware as a part of an open service area with a password request; and

if the open request succeeds, causing the system firmware to move a SETMAX boundary to allow access to the requested service area.

18. The method recited in Claim 13 wherein the step of closing the protected area comprises the step of:

once the calling process has completed its activities in the protected area 27, returning the SETMAX address to its original boundary using a close command.